

日本国特許庁  
JAPAN PATENT OFFICE

#2  
12-13-01



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年10月18日

出願番号

Application Number:

特願2000-317675

出願人

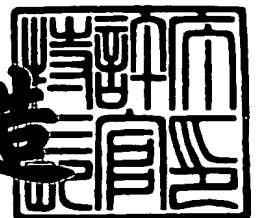
Applicant(s):

日本ピラー工業株式会社

2001年 8月 3日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3068196

【書類名】 特許願

【整理番号】 JP-NP1352

【提出日】 平成12年10月18日

【あて先】 特許庁長官 殿

【発明者】

    【住所又は居所】 大阪府大阪市淀川区野中南2丁目11番48号 日本ピ  
                        ラー工業株式会社内

    【氏名】 西村 志郎

【発明者】

    【住所又は居所】 大阪府大阪市淀川区野中南2丁目11番48号 日本ピ  
                        ラー工業株式会社内

    【氏名】 大野 泰一

【発明者】

    【住所又は居所】 大阪府大阪市淀川区野中南2丁目11番48号 日本ピ  
                        ラー工業株式会社内

    【氏名】 田中 勝也

【発明者】

    【住所又は居所】 大阪府大阪市淀川区野中南2丁目11番48号 日本ピ  
                        ラー工業株式会社内

    【氏名】 森田 隆嗣

【特許出願人】

    【識別番号】 000229737

    【氏名又は名称】 日本ピラー工業株式会社

【代理人】

    【識別番号】 100082474

    【弁理士】

    【氏名又は名称】 杉本 丈夫

    【電話番号】 06-6201-5508

【手数料の表示】

【予納台帳番号】 003263

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9714321

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークサービス

【特許請求の範囲】

【請求項 1】 サービス提供者は、予め、ユーザ適格を確認したユーザに、当該ユーザが使用するクライアントコンピュータにインストールしうるユーザ識別ファイルを提供し、クライアントコンピュータからのアクセス要求があった場合に、当該クライアントコンピュータに内在するユーザ識別ファイルの有無をブラウザ表示画面において確認し、ユーザ識別ファイルの存在が確認されたクライアントコンピュータからのアクセス要求に対してのみ特定のサービスを提供することを特徴とするネットワークサービス。

【請求項 2】 ユーザ識別ファイルは、これをインストールすることによって当該クライアントコンピュータの既存プログラムに何らの影響を及ぼさないものであって、ブラウザ表示画面においてその有無が確認されうるコンピュータ識別記号を具備するものであることを特徴とする、請求項 1 に記載するネットワークサービス。

【請求項 3】 コンピュータ識別記号は、複数のアスキー文字を羅列してなるものであることを特徴とする、請求項 2 に記載するネットワークサービス。

【請求項 4】 サービス提供者は、ユーザ識別ファイルを磁気媒体に格納してユーザに提供することを特徴とする、請求項 1、請求項 2 又は請求項 3 に記載するネットワークサービス。

【請求項 5】 サービス提供者は、ユーザが所有する一又は複数のコンピュータにユーザ識別ファイルをインストールすることを特徴とする、請求項 1、請求項 2、請求項 3 又は請求項 4 に記載するネットワークサービス。

【請求項 6】 ユーザは、自己の所有する一又は複数のコンピュータにユーザ識別ファイルをインストールすることを特徴とする、請求項 1、請求項 2、請求項 3 又は請求項 4 に記載するネットワークサービス。

【請求項 7】 ユーザ適格の確認は、サービス提供者とユーザとのサービス利用契約の締結によって行われることを特徴とする、請求項 1、請求項 2、請求項 3、請求項 4、請求項 5 又は請求項 6 に記載するネットワークサービス。

【請求項 8】 サービス利用契約が代理店契約であることを特徴とする、請求項 7 に記載するネットワークサービス。

【請求項 9】 ユーザ適格の確認は、サービス提供者によるユーザ識別ファイルのインストール時に行われることを特徴とする、請求項 5 に記載するネットワークサービス。

【請求項 10】 ユーザへの前記磁気媒体の提供は一般的な配送手段を介して行われ、当該磁気媒体のユーザへの配送完了をもってユーザ適格が確認されることを特徴とする、請求項 4 に記載するネットワークサービス。

【請求項 11】 サービス提供者は、ユーザを訪問して、前記磁気媒体の提供及びユーザ適格の確認を行なうことを特徴とする、請求項 4 に記載するネットワークサービス。

【請求項 12】 サービス提供者は、アクセス権を認めようとする全てのユーザ又は複数のユーザに対して、同一内容のユーザ識別ファイルを提供することを特徴とする、請求項 1、請求項 2、請求項 3、請求項 4、請求項 5、請求項 6、請求項 7、請求項 8、請求項 9、請求項 10 又は請求項 11 に記載するネットワークサービス。

【請求項 13】 特定のサービスを享受するユーザ専用画面へのログイン条件として、ユーザ固有の機密情報を含まないユーザ情報の入力を要求することを特徴とする、請求項 1、請求項 2、請求項 3、請求項 4、請求項 5、請求項 6、請求項 7、請求項 8、請求項 9、請求項 10、請求項 11 又は請求項 12 に記載するネットワークサービス。

【請求項 14】 前記ユーザ情報は、サービス提供者から提示されたユーザ ID 及び／又はパスワードであることを特徴とする、請求項 13 に記載するネットワークサービス。

【請求項 15】 前記ユーザ情報の入力画面からユーザ専用画面へのログイン操作に伴って、コンピュータ識別記号の有無確認が開始されることを特徴とする、請求項 13 又は請求項 14 に記載するネットワークサービス。

【請求項 16】 コンピュータ識別記号の存在が確認されたときにのみ、入力されたユーザ情報をデータベースに保存されたユーザ情報と照合して、その整

合が確認されることにより認証情報の入力画面からユーザ専用画面へのログインを許可することを特徴とする、請求項 1 3、請求項 1 4 又は請求項 1 5 に記載するネットワークサービス。

【請求項 1 7】 ユーザ識別ファイルの存在情報はクッキーに保持され、そのクッキーにおける保持情報は当該ネットワークへの接続終了によって消失することを特徴とする、請求項 1、請求項 2、請求項 3、請求項 4、請求項 5、請求項 6、請求項 7、請求項 8、請求項 9、請求項 1 0、請求項 1 1、請求項 1 2、請求項 1 3、請求項 1 4、請求項 1 5 又は請求項 1 6 に記載するネットワークサービス。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、クライアントコンピュータからインターネット等のネットワークを介してサーバコンピュータに接続することによりアイテムの購入注文やデータベース使用等の各種サービスを受けることができるネットワークサービスに関するものである。

【0 0 0 2】

【従来の技術】

従来から、ネットワークを通じて種々のサービスが提供されており、例えば、ユーザは、自己が使用するパソコン（パーソナルコンピュータ）等からインターネットを通じてサービス提供者のホームページにアクセスすることにより、アイテムの注文、購入やデータベースの使用、閲覧等の特定のサービスを受けることができる。

【0 0 0 3】

かかるネットワークサービスにあっては、特定のサービスはホームページにリンクされた特定のウェブページ（以下「ユーザ専用画面」という）において提供されるが、不正なアイテム注文、データベース使用等を防止するために、サービス提供者は、ユーザ適格を確認できるユーザ情報、例えばユーザの住所、氏名、年齢、職業、勤務先、役職、性別、電話番号、ファックス番号、電子メールアドレス

レス、クレジットカード番号等のユーザ固有の機密情報やサービス提供者との間で設定されるユーザID及びパスワードを要求し、かかるユーザ情報が入力された場合にのみユーザ専用画面へのアクセスを許可するようにしている。

【0004】

【発明が解決しようとする課題】

しかし、このようなユーザ情報は、ネットワーク上で他人にインターセプトされる虞れがあり、不正使用されて多大な損害を受けることがある。特に、クレジットカード番号等のユーザ固有の機密情報は、サービス提供者にとっては一面識もないユーザ適格を確認する上で有効且つ便利なものであるが、他人が不正に知得、使用することによってユーザが受ける被害は極めて大きい。勿論、ユーザ情報を不正に知得した他人によるアクセスによりデータベースが破壊される等、サービス提供者にとっても大きな被害を受ける場合がある。

【0005】

従来からも、アクセス権の認証を複雑な暗号キーを使用して行なう等、種々のセキュリティシステムが提案されているが、ネットワーク上でユーザ（人）を特定することによってアクセス権の認証を行なう以上、ネットワーク上に提供されるユーザ情報の漏洩阻止は困難であるし、ユーザ情報のインターセプトを有効に防止できるような超高度のセキュリティシステムは、その開発、インフラ構築等に多大な労力、コストを要するため、資金力のない一般的なサービス提供者にとっては到底採用できない。

【0006】

本発明は、このような問題を生じることなく、特定のサービスをユーザ及びサービス提供者の何れにとっても安全に提供、享受しうるネットワークサービスを提供することを目的とするものである。

【0007】

【課題を解決するための手段】

本発明は、上記の目的を達成すべく、サービス提供者は、予め、ユーザ適格を確認したユーザに、当該ユーザが使用するクライアントコンピュータにインストールしうるユーザ識別ファイルを提供し、クライアントコンピュータからのアク

セス要求があった場合に、当該クライアントコンピュータに内在するユーザ識別ファイルの有無をブラウザ表示画面において確認し、ユーザ識別ファイルの存在が確認されたクライアントコンピュータからのアクセス要求に対してのみ特定のサービスを提供することを特徴とするネットワークサービスを提案する。すなわち、このネットワークサービスにあっては、アクセス権の認証を、ユーザ（人）を特定することによって行わず、クライアントコンピュータそのものを特定することによって行なうものであり、アクセス要求に対してユーザ固有の機密情報を認証条件としないものである。特定のサービスは、一般には、インターネット（WWW（ワールド・ワイド・ウェブ）等）を通じて提供されるもの（例えば、アイテムの注文、購入（一般的な配送手段（宅配便、郵送、運送等）により配送される物理的な製品、商品や電子的手段（インターネット、電子メール等）により配送（ダウンロード等）される電子商品（デジタルデータ、アプリケーションソフト、音楽データ等）の注文、購入）やデータベース情報（アイテムの在庫情報等）の使用）であるが、インターネット以外のネットワーク（例えば、WAN等）を通じて提供されるものも含まれる。ユーザ識別ファイルの存在情報はクッキーに保持され、そのクッキーにおける保持情報は当該ネットワークへの接続終了（例えば、ホームページへのアクセス終了）と共に消失し、ネットワーク上から当該情報がインターセプトされるのを防止する。

## 【 0 0 0 8 】

かかるネットワークサービスにあって、ユーザ識別ファイルは、これをインストールすることによっては当該クライアントコンピュータの既存プログラムに何らの影響を及ぼさないものであって、ブラウザ表示画面においてその有無が確認されうるコンピュータ識別記号を具備するものである。このコンピュータ識別記号は、具体的には、複数のアスキー文字を羅列してなるものであり、ユーザ識別ファイルがインストールされたコンピュータを個性化する。ユーザ識別ファイルは、通常、ディスクット、CD-ROM等の磁気媒体に格納して、サービス提供者からユーザに提供される。磁気媒体のユーザへの提供は、一般的な配送手段（郵送等）を介して行なう他、サービス提供者（サービス提供者が雇用する従業者又はサービス提供者が委託する特定業者等を含む）がユーザを訪問して直接に行



なう。

【 0 0 0 9 】

また、ユーザ適格の確認は、サービス提供者とユーザとの間にサービス利用契約（例えば、代理店契約等）が締結される場合には、その締結をもって行なうことができる。また、ユーザ識別ファイルが、上記した如く、磁気媒体に格納してユーザに提供される場合には、磁気媒体の提供行為そのものがユーザ適格の確認行為を兼用する。すなわち、磁気媒体が郵送等の一般的な配送手段により配送される場合には、その配送完了により当該ユーザの住所、氏名等を確認することができ、当該配送完了をもってユーザ適格が確認される。また、サービス提供者がユーザを訪問して磁気媒体をユーザに提供するときは、サービス業者はユーザと面談することができ、これによってユーザ適格を、サービス利用契約の締結を行なう場合と同様に、確実に判断することができる。

【 0 0 1 0 】

また、ユーザ識別ファイルのインストールは、ユーザ適格が確認されたユーザ又はサービス提供者によって行われ、ユーザが当該ネットワークサービスに使用しようとする一又は複数のコンピュータに対して行われる。インストール操作は、上記した磁気媒体を使用して、ユーザ自身が行なう他、サービス提供者が行なう。サービス提供者によるインストール操作は、サービス利用契約時又は磁気媒体の提供時に行なうことができる。サービス提供者によるインストールは、ユーザとの面談によるユーザ適格の確認を兼ねることから、ユーザがコンピュータ知識に乏しく、ユーザ自身がインストール操作を行ない難い場合は勿論であるが、そうでない場合にも、ユーザ適格の確認上、サービス提供者がインストール操作を行なうことが好ましい。なお、サービス内容又はユーザ適格によっては、インストールすべきコンピュータの数を制限することも好ましい。かかる制限を行なう場合には、サービス提供者はユーザ識別ファイルを格納した磁気媒体をインストール後に回収する。また、ユーザ識別ファイル（特に、コンピュータ識別記号）は、当該ネットワークサービスによるサービスを享受する全てのユーザ又はグループ化された複数のユーザに対して同一内容のものとすることができる。このようにする場合には、セキュリティ上、定期的にユーザ識別ファイルのバージョ

ン変更（コンピュータ識別記号の変更）を行なうことが好ましい。

【0011】

ところで、ネットワークサービスにあって、ユーザ個々のニーズに応じたサービスを提供する必要がある、サービス提供画面であるユーザ専用画面をユーザ毎に又はグループ化されたユーザ毎にカスタマイズさせることが望ましい場合がある。

【0012】

このような場合等にあつては、特定のサービスを享受するユーザ専用画面へのログイン条件として、ユーザに対して、ユーザ識別ファイルのインストールに加えて、ユーザ情報の入力を求めることができる。かかるユーザ情報は、ネットワーク上での漏洩がユーザに不利となるようなユーザ固有の機密情報（ユーザの年収、クレジットカード番号等）は含まれず、一般には、サービス提供者によって提示されたユーザID及びパスワードの両方又は一方である。ユーザIDによってユーザ専用画面を、ユーザに応じてカスタマイズすることができ、ユーザ個々のニーズに応じた決め細やかなサービスを提供することができる。

【0013】

かかる場合、ユーザ情報の入力画面からユーザ専用画面へのログイン操作に伴って、ユーザ識別ファイル（コンピュータ識別記号）の有無確認が開始され、サーバコンピュータは、ユーザ識別ファイルの存在が確認されたときにのみ、入力されたユーザ情報（ユーザID等）をデータベースに保存されたユーザ情報と照合して、その整合が確認されることにより認証情報の入力画面からユーザ専用画面へのログインを許可する。すなわち、ユーザID等のユーザ情報の整合確認処理を、ユーザ識別ファイルの存在が確認された後に行なうことにより、仮にネットワーク上で当該ユーザ情報がインターセプトされ、そのユーザ情報を使用した不正なアクセス要求があったときにも、その要求を確実に拒絶することができ、セキュリティを確保することができる。

【0014】

【発明の実施の形態】

本発明の実施の形態におけるネットワークサービスは、図1に示す如く、ユー

ザが所有するクライアントコンピュータ 1 とサービス提供者が所有、管理するサーバコンピュータ 2 とをネットワーク（インターネット） 3 を介して接続したクライアント・サーバシステムによって行われる。

## 【 0 0 1 5 】

クライアントコンピュータ 1 は、ユーザが所有する設置型のコンピュータ（デスクトップ型パソコン等）又は携帯端末（ノートパソコン等）であり、WWWブラウザ（例えば、マイクロソフトのインターネット・エクスプロラやネットスケープのナビゲータ等）及びディスプレイ等を装備しており、インターネット 3 に所定のURLを送出することにより、このURLにより特定されるリソース（ハイパーテキスト）を取得し、ディスプレイ上に所望の画像表示を行なう。当該ネットワークサービスによる特定のサービスを利用できるクライアントコンピュータ 1 には、後述する如く、コンピュータ識別記号を有するユーザ識別ファイルがインストールされている（以下、ユーザ識別ファイルがインストールされたコンピュータとインストールされていないコンピュータとを区別する必要がある場合には、前者を「特定コンピュータ」といい、後者を「不特定コンピュータ」という）。また、特定コンピュータを使用するユーザ（以下、不特定コンピュータを使用するユーザとを区別する必要がある場合には「特定ユーザ」という）には、サービス提供者からユーザ情報（ID及びパスワード）が提示されている。なお、一のユーザに対して認められる特定コンピュータ 1 の数は、サービス提供者が制限することができるが、かかる制限がなく、当該ユーザがサービス使用条件等に応じて任意に設定することを許容する場合もある。例えば、本店のコンピュータとこれにWAN等で接続されていない支店や営業所のコンピュータとを夫々特定コンピュータとして使用したい場合、又はユーザの従業者が任意の場所からノートパソコン等の携帯端末によりアクセスしたい場合等があるからである。

## 【 0 0 1 6 】

サーバコンピュータ 2 は、WWWサーバ 4 及びデータベース 5 等を具備するコンピュータシステムであり、必要に応じてLAN，WANによるネットワークシステムが含まれる。サーバ 4 はインターネット 3 に接続されており、ホームページ表示ファイルを具備する。なお、サーバコンピュータ 2 には、必要に応じて、

一般的なセキュリティシステム（ファイアウォール等）を付設することができる。ホームページ表示ファイルは、複数階層のウェブページ（ユーザ情報の入力画面、ユーザ専用画面等）で構成されるホームページをブラウザに送出する処理、コンピュータ識別記号の取得、保持処理、コンピュータ識別記号の判別処理及びユーザ情報の照合、確認処理を行なうプログラムで構成される。コンピュータ識別記号の取得、保持処理にあつては、特定コンピュータ 1 からのホームページアクセス時にユーザ識別ファイルによって当該コンピュータ 1 に付与されたコンピュータ識別記号を自動取得し、これをクッキー機能の利用によりブラウザ表示画面上で暗黙に保持する。コンピュータ識別記号の判別処理にあつては、ブラウザ表示画面上で取得、保持されるコンピュータ識別記号の有無を判別し、ユーザ情報の照合、確認処理にあつては、コンピュータ識別記号の存在が確認されたときにおいてユーザにより入力されたユーザ情報であるユーザ ID 及びパスワードをデータベース情報（データベース 5 に保持された ID、パスワードに関するユーザ情報）と照合し、両者が整合した場合にユーザ専用画面からデータベース 5 へのアクセスを許容する。

## 【 0 0 1 7 】

特定コンピュータ 1 には、サービス提供者から提供されるユーザ識別ファイルがインストールされる。このユーザ識別ファイルは、ディスク（フロッピディスク）や CD-ROM 等の適宜の磁気媒体に格納されており、その特定コンピュータ 1 へのインストールは当該磁気媒体を使用して行なわれる。ユーザ識別ファイルは、適当数のアスキー文字を羅列してなるコンピュータ識別記号（テキストファイル）及びこれをブラウザ表示画面上で読み取るためのダイナミック・リンク・ライブラリ（DLL）を含むものであり、磁気媒体には、必要に応じて、ユーザ識別ファイルの他、これを特定コンピュータに組み込むためのインストール用ウィザードプログラムが格納される。ユーザ識別ファイルは、特定コンピュータ 1 に他のコンピュータ（不特定コンピュータ）と区別するための独自のコンピュータ識別記号（認証記号）を付与する機能を有するものであり、これをインストールすることによっては、当該コンピュータ 1 の既存プログラム（オペレーティング・システム（Windows 98, MS-DOS, OS/2 等）やアプ

リケーションプログラム等）に何らの影響を与えないものであり、一般に、ユーザによるファイル操作が行われないディレクトリないしファイル（例えば、システムファイル）に格納，保持される。

## 【 0 0 1 8 】

ユーザ識別ファイルの特定コンピュータ 1 へのインストールは、サービス提供者によるユーザ適格の確認を兼ねる意味で且つ前記磁気媒体の不正使用の防止を図るために、原則として、サービス提供者が行なう。すなわち、サービス提供者がユーザを訪問して、当該ユーザが使用しようとするコンピュータ 1 にインストールすることにより、サービス提供者はユーザが特定ユーザとしての適格性（ユーザ適格）を具備する者であるか否か（当該ネットワークサービスを適正に利用できる者であるか否か）を直接に判断することができ、爾後の電子商取引等の安全が保証される。一方、ユーザが代理店契約等のサービス利用契約の締結により信用できる者であることが保証されている場合には、前記磁気媒体を郵送，宅配便等の一般的な配送手段により当該ユーザに配送し、ユーザ自らがユーザ識別ファイルのインストールを行なう。この場合においても、特定ユーザがコンピュータ操作に熟知しない場合には、当該ユーザからの要請等により、サービス提供者がユーザ識別ファイルのインストールを行なう。

## 【 0 0 1 9 】

而して、本発明に係るネットワークサービスにあっては、図 2 に示す如きルーチンにより、特定ユーザに特定のサービス（製品発注，在庫照会等のデータベース使用サービス）が提供される。

## 【 0 0 2 0 】

すなわち、ユーザ識別ファイルがインストールされた特定コンピュータ 1 からウェブブラウザを起動し、サービス提供者のホームページにアクセスし、ホームページ画面を特定コンピュータのディスプレイに表示する。ホームページ画面には、ユーザ専用画面へのログインボタンがあり、これをクリックすることにより、ユーザ情報の入力画面が表示される。特定ユーザは、この入力画面において、予めサービス提供者から提示されたユーザ ID 及びパスワードを入力する。そして、当該入力画面に表示されるログインボタンをクリックすることにより、入力さ

れたユーザIDによってカスタマイズされたユーザ専用画面が表示され、データベース5へのアクセスが許容される。

【0021】

このとき、ユーザ専用画面へのログインは、ユーザ識別ファイルがインストールされた特定コンピュータ1によるアクセスに対してのみ行われ、不特定コンピュータからのアクセスに対しては拒否される。

【0022】

すなわち、ユーザ情報の入力画面からユーザ専用画面へのログイン操作（ログインボタンのクリック）が行われると、ブラウザ表示画面上において、当該コンピュータ1におけるコンピュータ識別記号の有無が判別、確認される。サーバコンピュータ2は、コンピュータ識別記号の存在が確認されると、データベース5に保存されているユーザ情報と入力されたユーザID及びパスワードとを照合する。そして、これらが整合した場合には、ユーザ専用画面を表示し、データベース5へのアクセスを許可する。ユーザ専用画面は、ユーザIDによってカスタマイズされたものであり、特定ユーザが所望する一又は複数のセクションを有する。例えば、製品注文セクション、在庫情報セクション、発注製品の出荷情報セクション、データベースダウンロードセクション等である。一方、入力されたユーザID又はパスワードがデータベース情報と整合しない場合には、適当なエラー画面が表示され、ユーザ専用画面へのログインが拒否される。

【0023】

また、ユーザ専用画面へのアクセス要求が不特定コンピュータからなされた場合には、ブラウザ表示画面においてコンピュータ識別記号が確認されず、適当なエラー画面が表示され、ユーザ専用画面へのログインが拒否される。このとき、入力されたユーザ情報とデータベース情報との照合は行なわれない。すなわち、これらの情報照合は適正なコンピュータ識別記号の存在が確認された場合にのみ行なわれる。したがって、複数の不特定コンピュータを含む多数のコンピュータ1からのアクセスが同時に行なわれたときにも、不正アクセス（インターセプトされたユーザ情報（形式上、適正なユーザID、パスワード）を使用したアクセスを含む）を含めた全てのアクセスについて入力されたユーザID、パスワード

とデータベース情報との照合、整合判断を行なうようにする場合に比して、サーバコンピュータ 2 による処理負担（サーバ 4 への負荷）が軽減されて、サーバ能力を必要以上に高くしておく必要がなく、サーバコンピュータ 2 の小型化、低コストを図ることができる。

## 【 0 0 2 4 】

ところで、ユーザ ID やパスワードは、ブラウザの URL 指定ラインやステータスバー、更にはソースコードをみることによって判明可能なものであるから、HTML コマンドに精通している者であれば容易に知得することができ、他人により不正アクセスされる虞れがある。

## 【 0 0 2 5 】

しかし、上述したように、ユーザ ID、パスワードの正誤判断をコンピュータ識別記号の存在が確認された特定コンピュータ 1 からのアクセスに対してのみ行ない、不特定コンピュータ 1 からのアクセスに対してはユーザ ID、パスワードが適正なものである場合にもユーザ専用画面へのログインないしデータベース 5 へのアクセスが拒否されることから、仮にユーザ ID、パスワードが盗用されたときにも、サービス提供者及びユーザが不測の損害を被ることがない。また、ユーザ ID、パスワードは当該ネットワークサービスにおいてのみ使用できるものであるから、ユーザ固有の機密情報と異なって、他のネットワークサービス等において不正使用されることによりユーザ（特定ユーザ）が被害を受けることはない。

## 【 0 0 2 6 】

また、コンピュータ識別記号の存在することが確認されたときは、その確認情報はクッキーに保持され、その保持状態はユーザ専用画面を含めた当該ホームページに接続されている限り継続する。したがって、ユーザ専用画面に対してログイン、ログオフが繰り返されるような場合にも、その都度、コンピュータ識別記号の確認処理を行なうといった煩雑を回避することができる。しかし、クッキーによる保持は、セキュリティ上、当該ホームページへの接続終了（オンライン解除）と共に消滅する。

## 【 0 0 2 7 】

ところで、コンピュータ識別記号は、アスキー文字を羅列した簡単なテキストファイルではあるが故に、暗号ファイル等の特殊なファイルと異なって目立つものではないから、ネットワーク上から特定コンピュータ 1 に不正に侵入された場合にも注意を喚起することがなく、ハッキングされる虞れが極めて少ない。したがって、コンピュータ識別記号によるコンピュータ 1 の個性化はセキュリティ面において極めて有効なアクセス権認証手段たり得る。

## 【 0 0 2 8 】

以上のように、本発明に係るネットワークサービスにあっては、ユーザ専用画面へのアクセス権の認証を、ユーザ固有の機密情報等のユーザ情報によってユーザ（人）自体を識別するのではなく、ユーザが使用するコンピュータ 1 をこれに内在するコンピュータ識別記号により個性化することによって行なうから、ユーザ情報がネットワーク上でインターセプトされるような危険はなく、ユーザが不測の損害を被ることがない。また、サービス提供者にとっても、不正なアクセスが確実に防止され、データベース 5 への不正侵入等による損害を受けることがなく、ネットワークサービスを安全に行なうことができる。

## 【 0 0 2 9 】

ところで、アクセス権の認証をコンピュータの個性化により行なう手法として、ＩＣカードリーダーを使用することも考えられるが、アクセス権を確保しようとするコンピュータ毎にＩＣカードリーダーを設置する必要があり、ネットワークサービスを使用するためのイニシャルコストが高くなる問題がある。特に、ユーザのニーズやサービス内容によっては、ユーザが所有する複数のコンピュータからアクセスすることが必要となる場合には、それらのコンピュータ毎にＩＣカードリーダーを設置しなければならず、経済的な負担は膨大となる。

## 【 0 0 3 0 】

しかし、本発明に係るネットワークサービスでは、使用するコンピュータにユーザ識別ファイルをインストールするだけであり、ユーザ識別ファイルを格納した磁気媒体以外に格別の機器は必要とせず、アクセス権認証（コンピュータ識別記号の有無判断）に要するシステム構築も簡単且つ容易であり、大きな経済的負担を生じることなくユーザのニーズに十分に 대응することができる。また、ユーザ



識別ファイルを、一旦、インストールしておけば、アクセスの都度、ＩＣカードリーダを操作するといった手間も必要とせず、特定コンピュータ１としてノートパソコン等の携帯端末を使用する場合には、任意の場所からもサービスの提供を容易に受けることができる。

## 【 0 0 3 1 】

なお、本発明は上記した実施の形態に限定されるものではなく、本発明の基本原理を逸脱しない範囲において適宜に改良，変更することができる。

## 【 0 0 3 2 】

例えば、ユーザＩＤ及びパスワード等のユーザ情報は、ユーザ専用画面のカスタマイズ等を行なう上で必要であるが、前述したようにネットワーク上でインターセプトされ易いものであり、ネットワークサービスのセキュリティを確保する上ではさほど重要なものではない。したがって、提供サービスの内容（ユーザ専用画面の構成）が画一なものであり、ユーザに応じてカスタマイズする必要がない場合等には、ユーザＩＤ，パスワード等のユーザ情報の入力を要求せず、ユーザ識別ファイルをインストールしたコンピュータ１からのアクセス要求に対して無条件にアクセス権を認証するようにすることができる。例えば、図３に示す如く、ユーザ専用画面へのログイン操作（ログイン用画面におけるログインボタンのクリック等）が行なわれると、コンピュータ識別記号の有無をブラウザ表示画面上で確認し、コンピュータ識別記号の存在が確認された場合には、ユーザ専用画面へのログインないしデータベースへのアクセスを許容する。かかる場合においても、コンピュータ識別記号はクッキー保持し、その保持情報はホームページへの接続終了により消滅する。一方、コンピュータ識別記号の存在が確認されない場合には、エラー画面を表示し、当該アクセスを拒否する。

## 【 0 0 3 3 】

本発明は、イントラネット，エクストラネット等の閉じられたネットワークを使用する場合、更にはＬＡＮ，ＷＡＮ上でのセキュリティを確保したい場合にも適用することが可能である。

## 【 0 0 3 4 】

## 【発明の効果】

以上の説明から理解されるように、本発明によれば、ネットワークサービスの提供、享受を安全に行なうことができる。しかも、複雑且つ高価なセキュリティシステムを必要とすることなく、ネットワークサービスのシステム構築を容易且つ安価になすことができる。

【図面の簡単な説明】

【図 1】

本発明に係るネットワークサービスを実施するためのシステム構成の一例を示すブロック図である。

【図 2】

本発明に係るネットワークサービスの実施の形態を示すフローチャート図である。

【図 3】

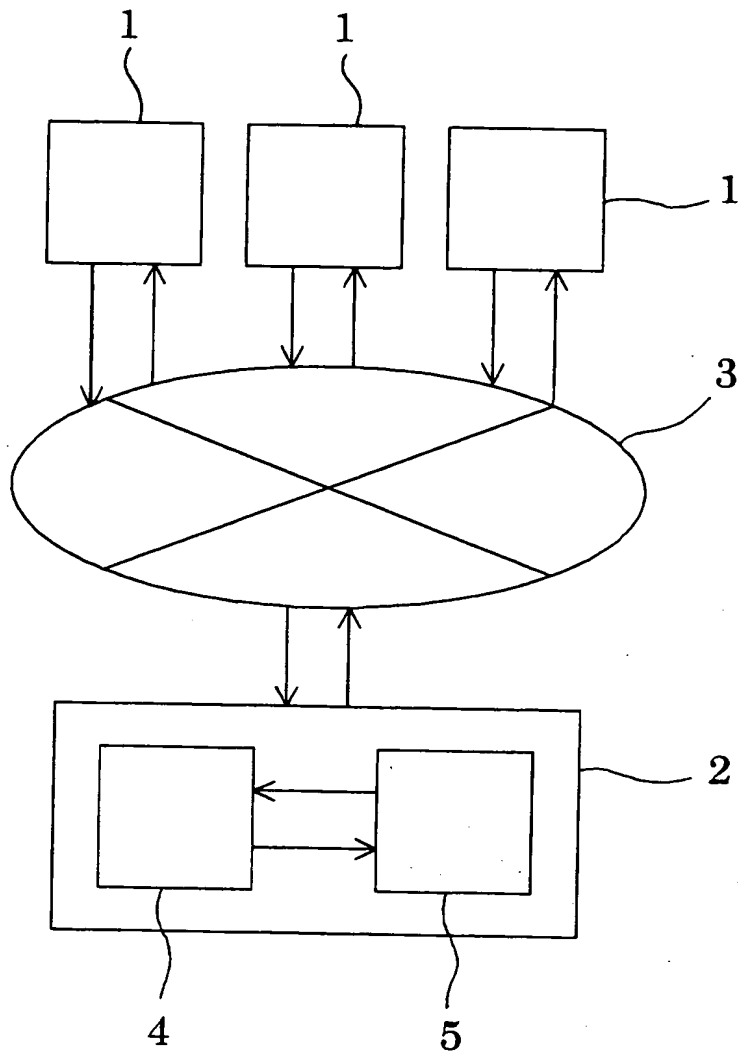
本発明に係るネットワークサービスの他の実施の形態を示すフローチャート図である。

【符号の説明】

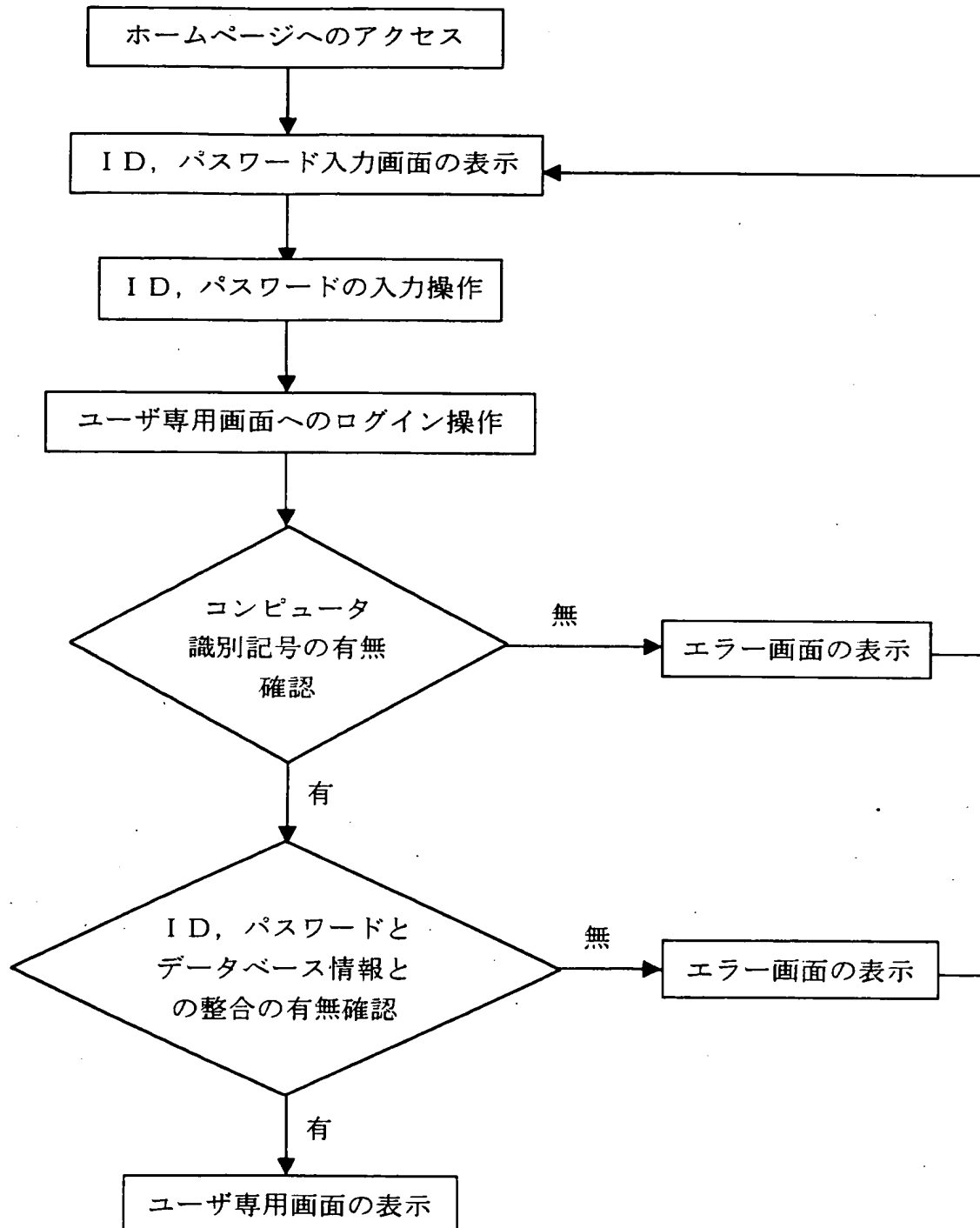
1 …クライアントコンピュータ、2 …サーバコンピュータ、3 …ネットワーク（インターネット）、4 …WWWサーバ、5 …データベース。

【書類名】 図面

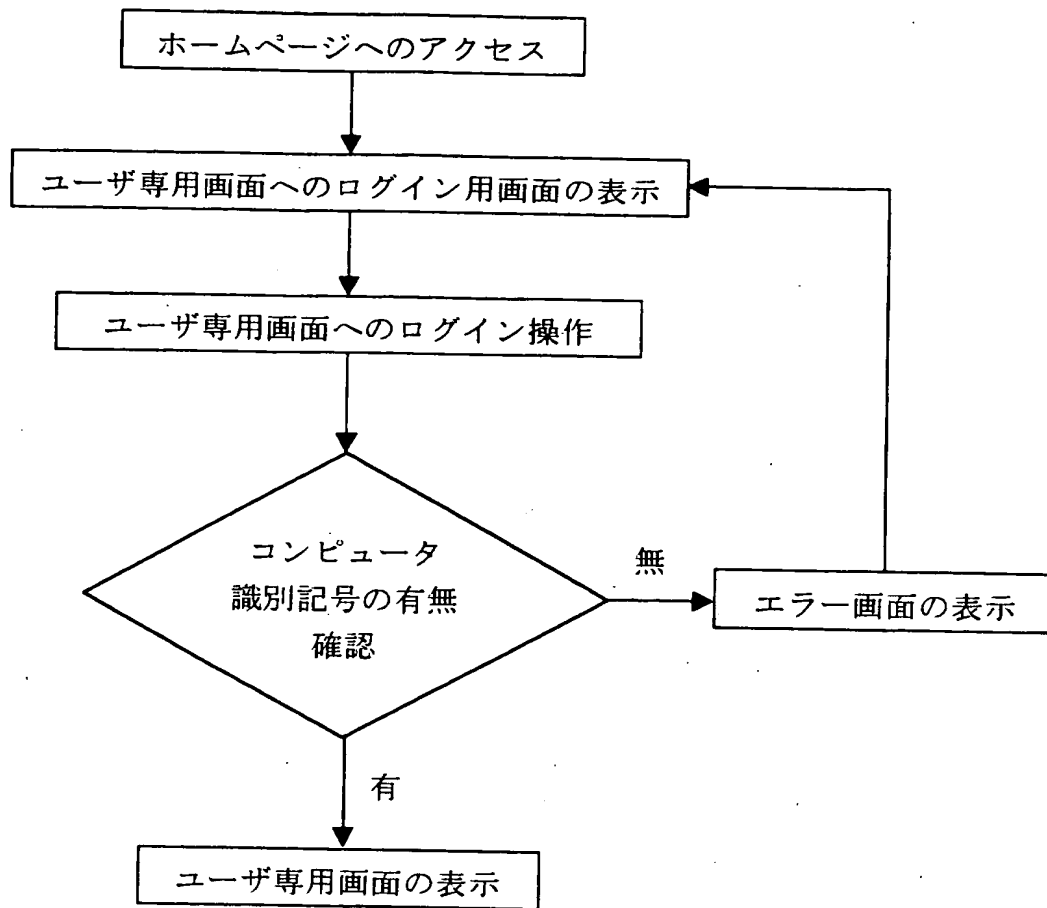
【図 1】



【図2】



【図3】



【書類名】                      要約書

【要約】

【課題】    特定のサービスをユーザ及びサービス提供者の何れにとっても安全に提供、享受しうるネットワークサービスを提供する。

【解決手段】    サービス提供者は、予め、ユーザ適格を確認したユーザに、当該ユーザが使用するクライアントコンピュータにインストールしうるユーザ識別ファイルを提供し、クライアントコンピュータからのアクセス要求があった場合に、当該クライアントコンピュータに内在するユーザ識別ファイルの有無をブラウザ表示画面において確認し、ユーザ識別ファイルの存在が確認されたクライアントコンピュータからのアクセス要求に対してのみ特定のサービスを提供する。ユーザ識別ファイルは、これをインストールすることによってはクライアントコンピュータの既存プログラムに何らの影響を及ぼさないものであって、ブラウザ表示画面においてその有無が確認されうるコンピュータ識別記号を具備する。

【選択図】                      図 2

出 願 人 履 歴 情 報

識別番号 [000229737]

1. 変更年月日	1990年 8月23日
[変更理由]	新規登録
住 所	大阪府大阪市淀川区野中南2丁目11番48号
氏 名	日本ピラー工業株式会社